

SYSTEM AND METHOD FOR ***UNIVERSAL IDENTIFICATION*** OF BIOLOGICAL HUMANS

Claims

What is claimed is:

1. A system for unique human identification and associated method and steps to capture and store data and DNA samples related to issue of Universal Identification Number (UIN) and a subsequent retrieval process for human identification and tracking involving various applications viz. medical emergencies, public domain interest profile, and confidential data by authorized agencies.
2. The method in accordance with claim 1, wherein said UIN as unique human identifier comprises of an association date in Year (four numerals), Month (two numerals) and Date (two numerals) format (YYYYMMDD). The association date is followed by up to first three characters of first name of a person and lastly followed by a computer generated four alphanumeric digits or characters. The UIN is such that is easy to recall and does not reveal any personal information of a confidential nature about the UIN holder and protects their privacy.

3. The method in accordance with claim 2, wherein the association date in the said UIN (as unique human identifier) comprises of a date that shall normally be the issue date for UIN. If the UIN issue date and associated name characters and the computer-generated alphanumeric characters for the issue date are non-available, then the association date is picked from those available from one of the previous dates in a time-horizon window, as explained in the attachments appended to this application.
4. The method in accordance with claim 3, wherein the association date for issue of the said UIN (as unique human identifier) is a date that shall normally be the issue date of the UIN, but in case of a clash with first three characters of the first name of the person for whom the UIN is under issue and non-availability of a suitable computer generated four alphanumeric characters, shall be successively previous date, searched and matched for issue of the UIN from the time-horizon window. This date shall be matched a day at a time, and the first previous date, that is closest to the UIN issue date, shall be picked.
5. The method in accordance with claim 2, wherein the first three characters of the first name of a person are the first three characters of a given name. In cases of non-availability of the first three characters of the first name, for reasons like the first name being shorter than three characters, the remaining

characters of the first name shall be filled up by a computer-generated alphabetical sequence.

6. The method in accordance with claim 2, wherein the first three characters of the first name of a person are the first three characters of a given name. In cases of non-availability of the first three characters of the first name, for reasons like if the first name is not given owing to cultural or religious traditions or any other reasons, all characters of the first name shall be filled up by a computer-generated alphabetical sequence.
7. The system in accordance with claim 2 wherein the said UIN comprises of a number representing a date and alphabetic characters representing name and alphanumeric characters representing a computer generated code. This arrangement is such that UIN comprises of, that stands in order for YYYY (Year), MM (Month), DD (Date), NNN (Name), CCCC (Computer-generated Code). YYYYMMDD represents collectively the association date, followed by NNN for first name and CCCC for computer-generated code.
8. In accordance with claim 1, the data that is collected and makes the basis for issue of the UIN shall be divided in 3 sections, namely Public, Health and Confidential.

9. In accordance with claim 8, the first section of data collected refers to Personal Information under the public domain and captures the fields of first, middle and last name, each one of these can be 40 characters in length. Name is followed by sex (male or female) and the desired contact address with contact telephone number and e-mail address. The data in public domain shall be accessible at all times to those who have the UIN followed by the public-domain access code. The public domain access-code is known to the UIN holder, who can pass it on to anyone with whom they desire to share this information. The public domain access would reveal no more information than what is normally available on a personal business card.

10. In accordance with claim 8, the second section of data collected refers to Personal Information under the medical domain. This data captures various fields like date of birth (in YYYYMMDD format), blood type (Group and RH in 2 or 3 character width as the case may be), immediate medical conditions that may require attention (within 100 characters), details of up to 3 most severe known allergies (each can take up to 40 characters), name and contact details of the current attending physician (Name, telephone, pager, address – within 100 characters width). Emergency contact person (relative or friend) with contact details and a back-up emergency contact, each one of these can be at-most 100 characters in length. The data under medical domain shall be accessible at all times on-line or by call only to authorized hospitals and registered medical practitioners who have the UIN followed by

the medical-domain access code. This data is made available to authorized viewers along with the public domain access data. Thus, the authorized viewers of medical domain data get all the relevant contact and emergency information that they may need to perform immediate treatment.

11. In accordance with claim 8, the third section of data collected refers to Personal Information under the confidential domain. This data contains all the information about UIN holder that is of a confidential nature and captures the fields as Country of birth with state, county, address of birth place, time of birth, all detailed addresses where the UIN holder has lived over 5 years, details of educational qualifications with institutes attended. Also, fields like complete present address with telephone number, country of residence, country of citizenship and details of all identifications issued so far and all numbers issued (viz. ITIN, SSN # etc.) and details of all passports and visas ever carried or issued. This data is periodically updated and the UIN holder has to own the responsibility to submit data for verification and update to the UIN issuing authority. The data related to educational qualifications including details of all schools attended, degrees or diplomas obtained, years of graduation, and subject of major. Professional affiliations, with all places of work and positions held, name of supervisor and address of workplace with dates worked. Professional societies, religious bodies or charitable and voluntary organization memberships and affiliations, positions held with dates since affiliated and addresses of the organizations. Details of birth marks and

identification marks. In addition, DNA Samples of the UIN holder shall be obtained (optionally), referenced with UIN and stored at a secure site in a protected environment.

12. In accordance with claim 11, the Personal Information under confidential domain is not disclosed to anyone who is not authorized to access this information. The authorized law-enforcement agencies would be able to access this information only by a combination of three keys. The three keys are - public information access code given by the UIN holder, the security access key (authorization code) known only to the law enforcement agencies that is periodically changed to maintain confidentiality, and a third access code key that is specifically issued to the law enforcement officer requesting the information. To get the third access code, the law enforcement personnel seeking information will need to identify themselves. In order to access the information, they need to have their own UIN available for identification and verification of their personal data to eliminate any attempts at fraud. Records of all confidential data sought would be maintained for a specific period.

13. In accordance with claim 1, the UIN holder shall be issued a UIN card that carries UIN number, name of the UIN holder, picture of the UIN holder, and a thumb impression for unique identification. Additional information that is vital for life saving purposes is printed on inside of the card and not visible from the outside. The UIN card is a folded card with four visible surfaces that can

hold data and information about the UIN holder. While two of the surfaces are covered in the inside fold, the two outer surfaces form the front and back of card.

14. In accordance with Claim 1, the UIN shall, work as part of an integrated scheme and system that aims at eliminating terrorism, protecting identity, prevent frauds and is an attempt towards making this world a better place to be by Global Integration. UIN shall be subsequently supplemented by a tracking device that operates through satellite and radio signals, and the integrated system would become HITS (Human Identification and Tracking System).

15. In accordance with Claim 1, a DNA sample shall be obtained from the UIN applicant and stored securely by the UIN issuing and identity protection agency in a secure environment. This DNA sample shall be released only in the case of the need to do so, upon appropriate request by a court of law under its authority and jurisdiction, in specific country that may normally be the residence nation of UIN holder, to settle matters related to identity fraud or eradication of terrorism. The DNA sample is referenced to the UIN.